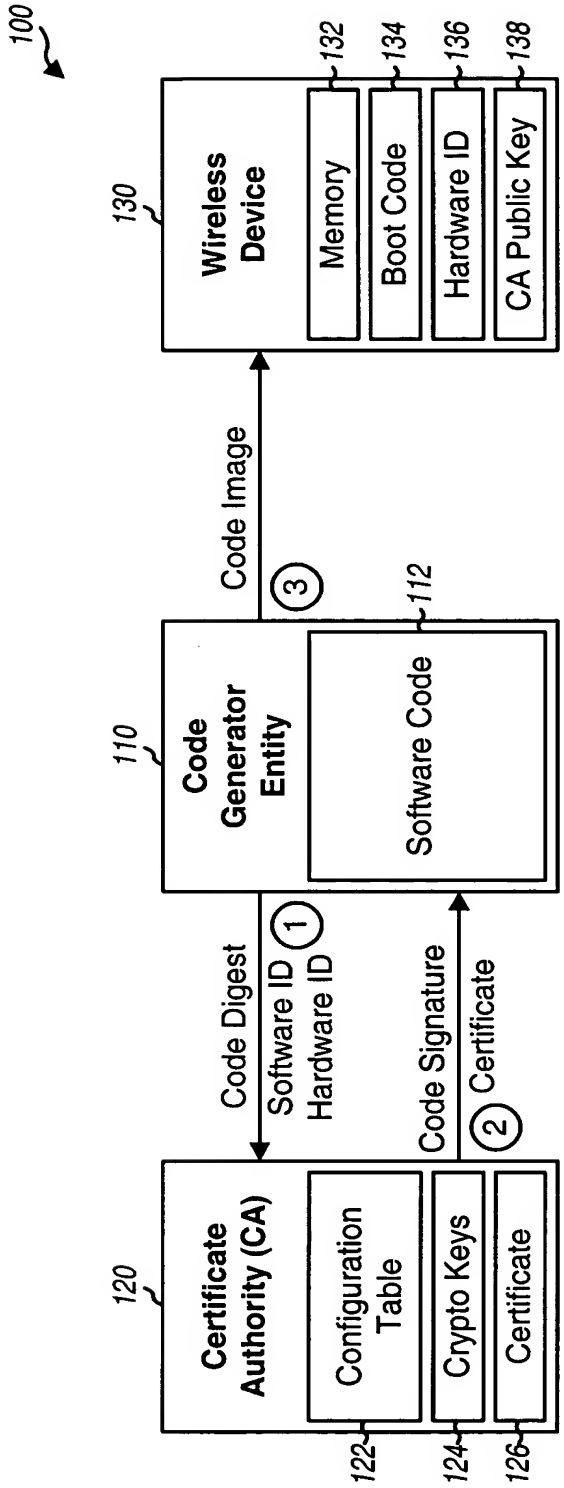
100
Certificate Authority (CA)
120
Configuration Table
122
Crypto Keys
124
Certificate
126
Code Generator Entity
110
Software Code
112
Wireless Device
130
Memory
132
Boot Code
134
Hardware ID
136
CA Public Key
138
Code Digest
Software ID
Hardware ID
1
Code Signature
2
Certificate
Code Image
3

FIG. 1

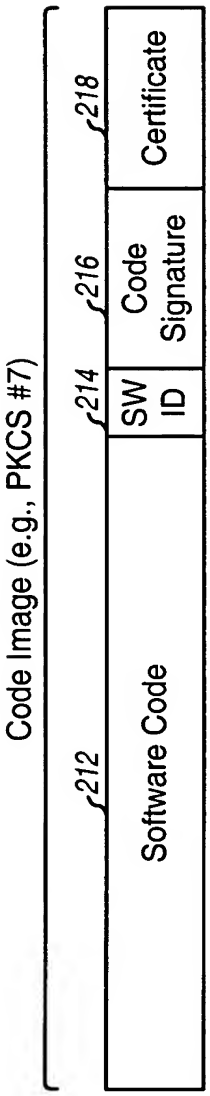
Code Image (e.g., PKCS #7)
Software Code
212
SW ID
214
Code Signature
216
Certificate
218

FIG. 2

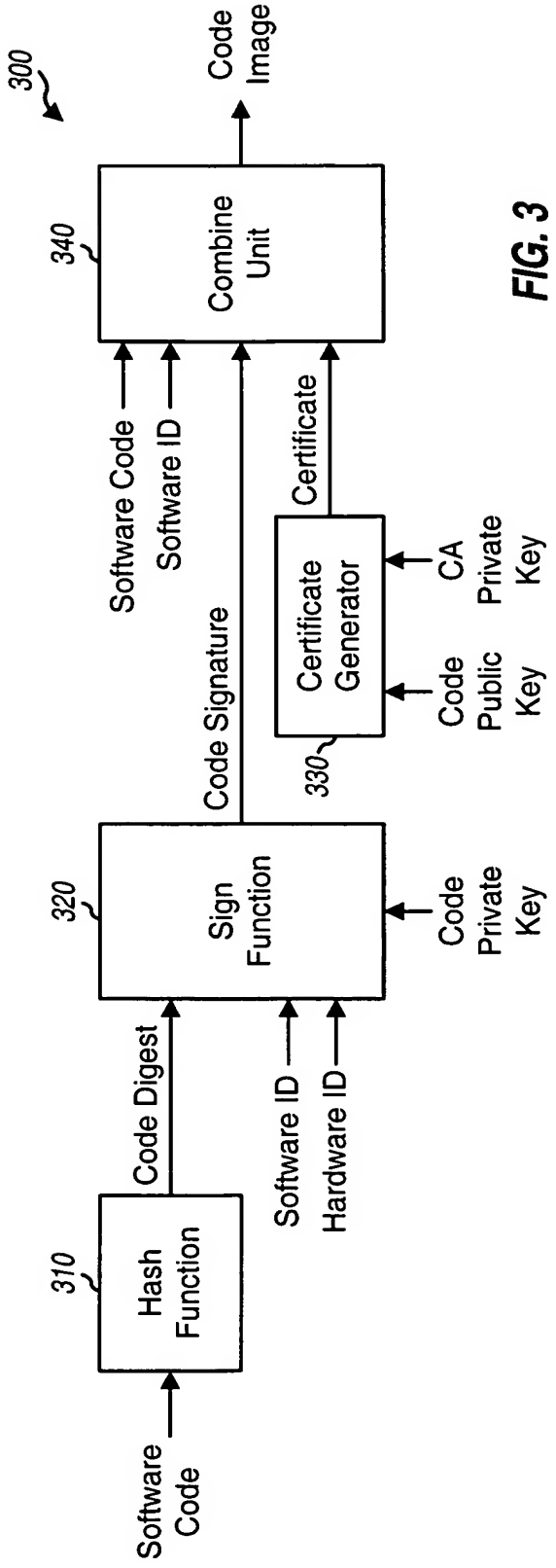
300
Code Image
340
Combine Unit
Software Code
Software ID
Certificate
Code Signature
Certificate Generator
CA Private Key
330
Code Public Key
320
Sign Function
Code Private Key
Code Digest
Software ID
Hardware ID
310
Hash Function
Software Code

FIG. 3

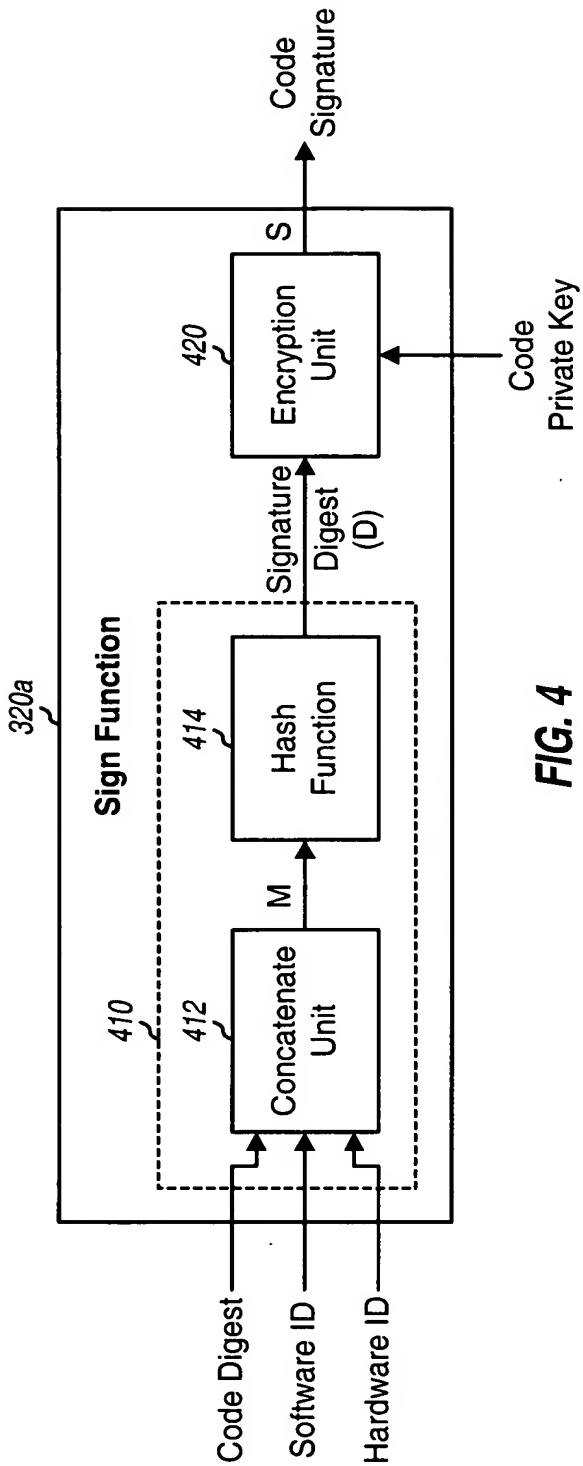
Code Signature
S
420
Encryption Unit
Code Private Key
Signature Digest (D)
320a
Sign Function
414
Hash Function
M
410
412
Concatenate Unit
Code Digest
Software ID
Hardware ID

FIG. 4

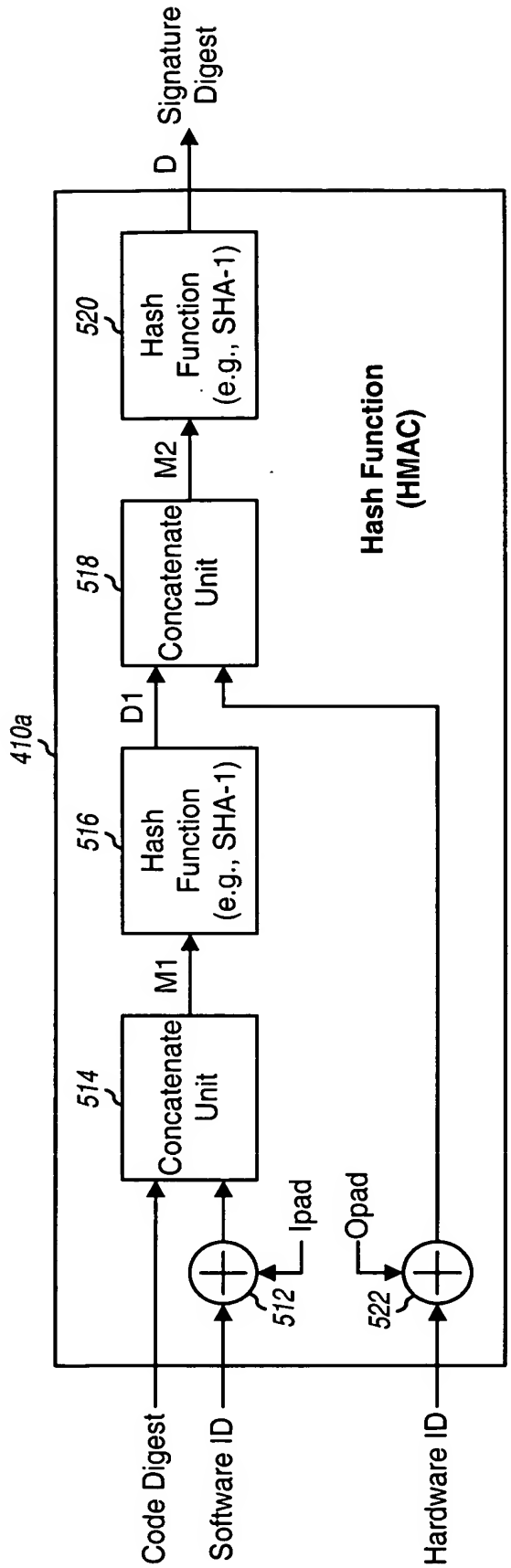
Code Digest
Software ID
Hardware ID
Ipad
Opad
512
522
514
Concatenate Unit
M1
516
Hash Function (e.g., SHA-1)
D1
518
Concatenate Unit
M2
520
Hash Function (e.g., SHA-1)
D
Signature Digest
410a
Hash Function (HMAC)

FIG. 5

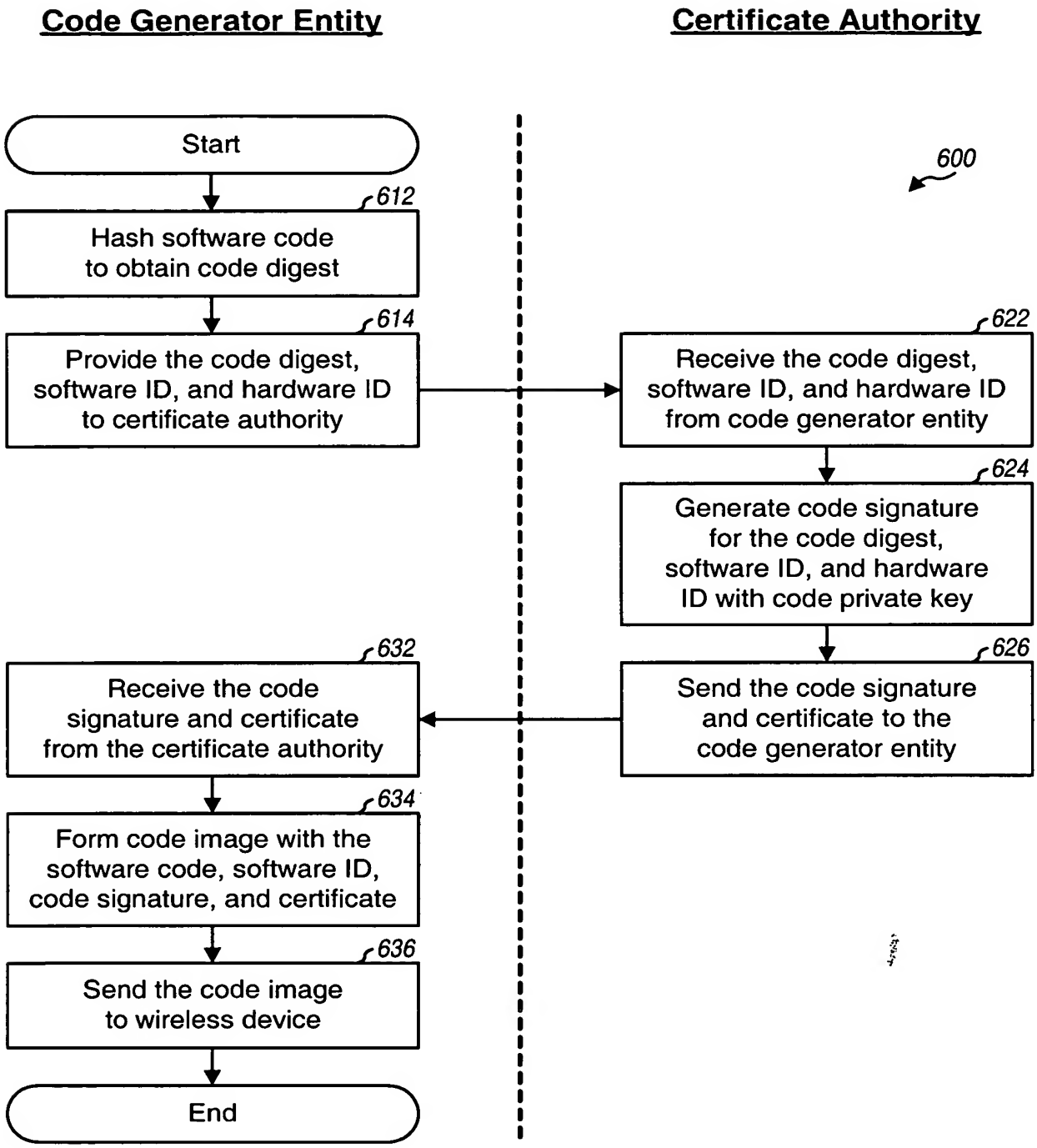
Code Generator Entity
Certificate Authority
600
Start
612
Hash software code to obtain code digest
614
Provide the code digest, software ID, and hardware ID to certificate authority
622
Receive the code digest, software ID, and hardware ID from code generator entity
624
Generate code signature for the code digest, software ID, and hardware ID with code private key
626
Send the code signature and certificate to the code generator entity
632
Receive the code signature and certificate from the certificate authority
634
Form code image with the software code, software ID, code signature, and certificate
636
Send the code image to wireless device
End

FIG. 6

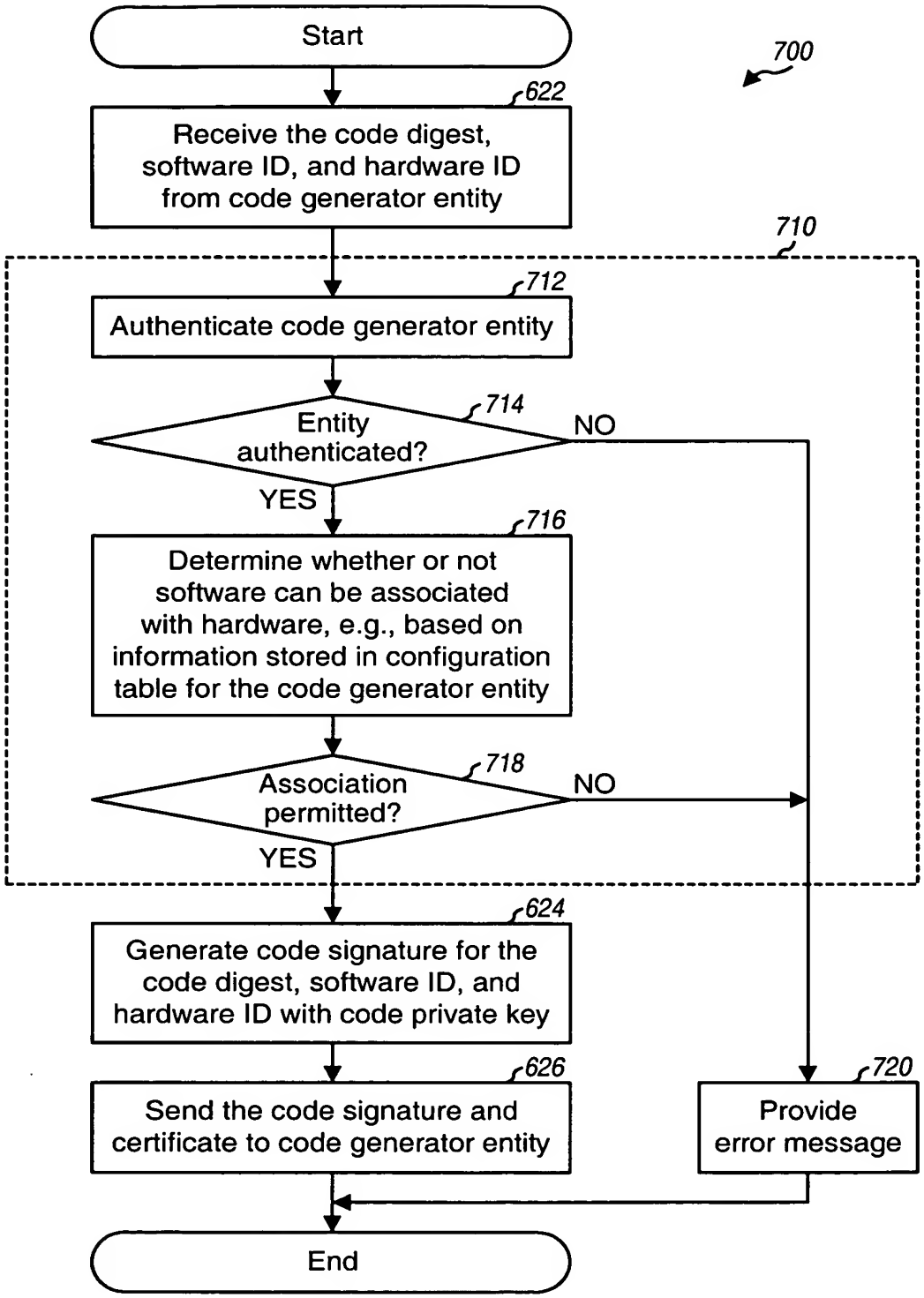
Start
700
622
Receive the code digest, software ID, and hardware ID from code generator entity
710
712
Authenticate code generator entity
714
Entity authenticated?
NO
YES
716
Determine whether or not software can be associated with hardware, e.g., based on information stored in configuration table for the code generator entity
718
Association permitted?
NO
YES
624
Generate code signature for the code digest, software ID, and hardware ID with code private key
626
Send the code signature and certificate to code generator entity
720
Provide error message
End

FIG. 7

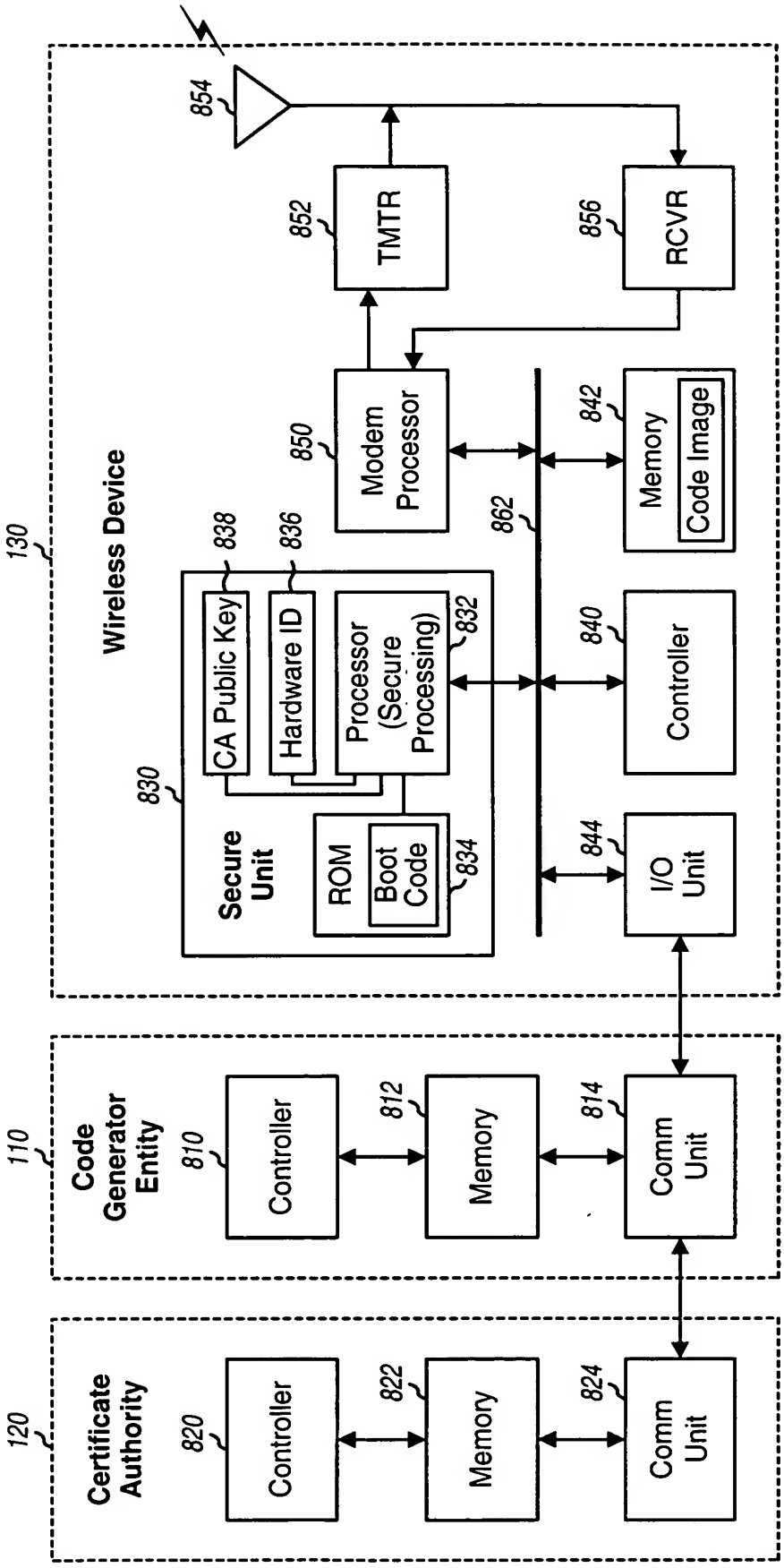
Certificate Authority
120
820
Controller
822
Memory
824
Comm Unit
Code Generator Entity
110
810
Controller
812
Memory
814
Comm Unit
Wireless Device
130
854
852
TMTR
856
RCVR
850
Modem Processor
862
842
Memory
Code Image
840
Controller
844
I/O Unit
Secure Unit
830
838
CA Public Key
836
Hardware ID
832
Processor (Secure Processing)
ROM
Boot Code
834

FIG. 8

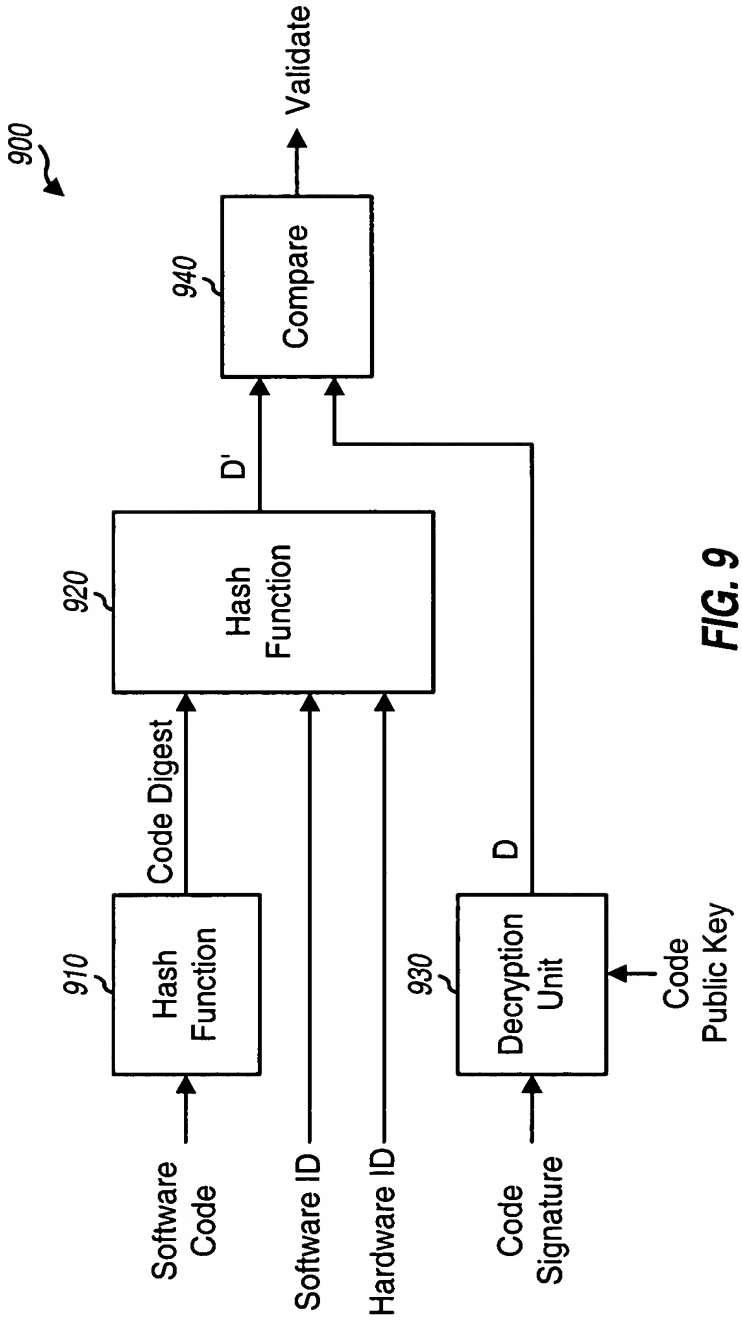
900
Validate
940
Compare
D'
920
Hash Function
Code Digest
910
Hash Function
Software Code
Software ID
Hardware ID
D
930
Decryption Unit
Code Public Key
Code Signature

FIG. 9

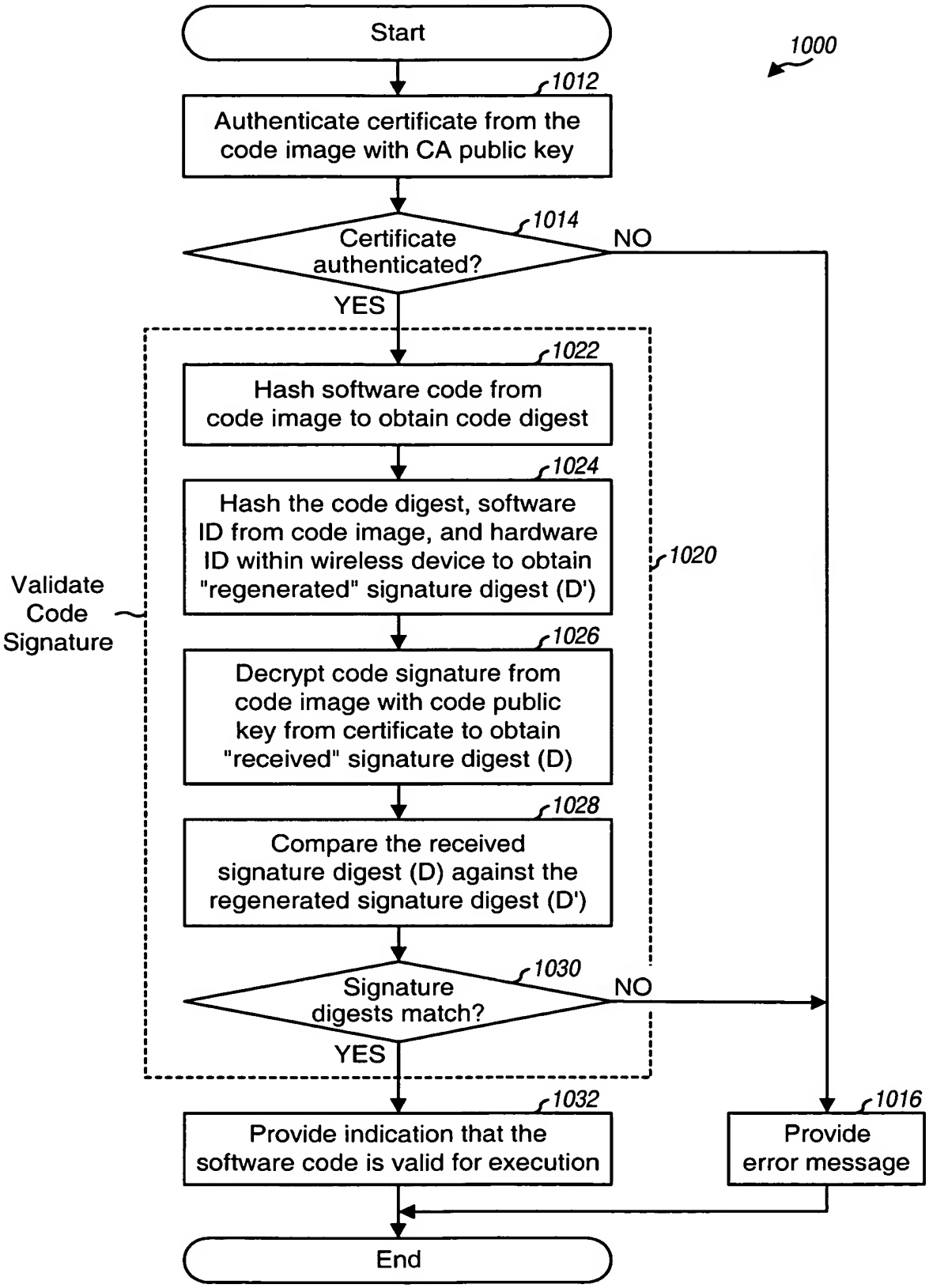
Start
1000
1012
Authenticate certificate from the code image with CA public key
1014
Certificate authenticated?
NO
YES
1022
Hash software code from code image to obtain code digest
1024
Hash the code digest, software ID from code image, and hardware ID within wireless device to obtain "regenerated" signature digest (D')
1020
Validate Code Signature
1026
Decrypt code signature from code image with code public key from certificate to obtain "received" signature digest (D)
1028
Compare the received signature digest (D) against the regenerated signature digest (D')
1030
Signature digests match?
NO
YES
1032
Provide indication that the software code is valid for execution
1016
Provide error message
End

FIG. 10